有扩展的前景//看看他们有没有接着写？

Mitigating Blackhole Attacks in a Hybrid VDTN

Yinghui Guo, Sebastian Schildt, Tobias Pögel, Stephan Rottmann and Lars Wolf
Institute of Operating Systems and Computer Networks
Technische Universität Braunschweig
Braunschweig, Germany
Email: [guo|schildt|poegel|rottmann|wolf]@ibr.cs.tu-bs.de

***Abstract*—In the past we presented a delay tolerant network that used public buses and trams in the city of Braunschweig to monitor air pollution. Today, as smartphones are becoming computationally more powerful and offer a variety of communication interfaces, it becomes attractive to investigate whether smartphones and vehicular nodes can cooperate with each other, forming a network that can provide better quality of service to applications. In this paper, we evaluate the feasibility of creating an integrated Delay- and Disruption-Tolerant Network (DTN) consisting of smartphones and the public transportation system. Most importantly we propose a Misbehavior Detection System (MDS) to protect the security of the hybrid network. The evaluation results show that our MDS is able to efficiently detect attackers and defend the hybrid network against the interference of malicious nodes.**

I. Introduction

Nowadays vehicles are becoming increasingly intelligent and the majority will soon be equipped with short-range radios and capable of communicating with other vehicles nearby. These vehicles will be an enabler for a wide range of applications including real-time traffic monitoring, environment monitoring and interactive communications between vehicles.

Some specialized applications have already been implemented for vehicular networks. Using buses or motorcycles, DakNet [1] and KioskNet [2] proposed a store-and-forward vehicular network to provide services such as e-mail or transfer of educational materials in rural environments. With the help of buses equipped with off-the-shelf communication hardware, DieselNet [3] built a versatile testbed for evaluating the communication performance among vehicles.

These examples show, that vehicular networks are a very promising communication system. Despite having a lot of potential, vehicular networks are also one of the most challenging networks. In vehicular networks, persistent connectivity among vehicular nodes cannot be guaranteed everywhere. When the network presents scarce transmission opportunities and intermittent connectivity, it is difficult to forward packets to their destinations. Therefore all mentioned applications are based on the idea of Delay- and Disruption-Tolerant Networks (DTNs), where a packet in the network will be sent over an existing link and buffered at a node until a connection to a suitable next hop is established. Using these delay-tolerant methods, we will create a Vehicular Delay- and Disruption-Tolerant Network (VDTN) until a high penetration of networked vehicles is achieved.

978-1-4799-4786-7/14/$31.00 ©2014 IEEE

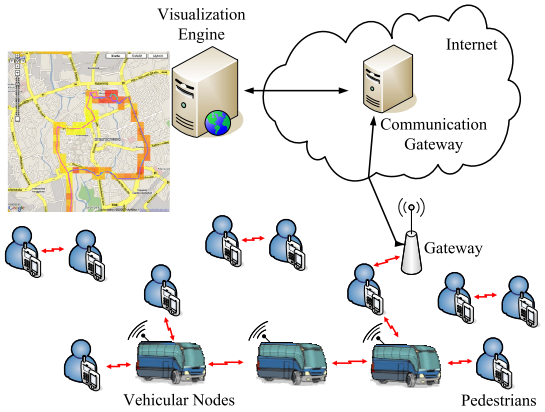

Figure 1. The hybrid urban communication network

In a former project [4], we implemented a DTN using the public transportation system to transport air pollution data. Later in the "Optracom" project[1], the system was extended to also include trams. Real-hardware was developed and deployed on trams and new applications such as transporting timetables or tourist information to interactive displays at tram stops have been introduced.

With the rapid development and proliferation of intelligent mobile devices such as smartphones, pedestrians carrying these devices might be used to act as networked nodes [5] enabling communication even when no other networking infrastructure is available. Hence in this paper, we propose a hybrid urban communication network with buses, trams and pedestrians working together (see Figure 1). We will evaluate the performance of the system when nodes with different characteristics exist in the network, and specially focus on the security issue of malicious and faulty nodes within this network.

Considering opportunistic connections and high mobility of nodes in VDTNs, traditional methods for detecting malicious behavior are difficult to apply to VDTNs. Most approaches rely on observing data forwarding directly, such as the Watchdog detection system [6] or CONFIDANT [7]. In our earlier works we proposed a Misbehavior Detection System (MDS) [8] based on encounter records [9], using indirect observation of events. We introduced a classifier based on clustering in [10] to make the MDS work without a long training phase or prior knowledge about the application. In

[1]Opportunistic Public Transport Communication http://www.optracom.de/

Figure 2. The DTN hardware for a tram

this work we will evaluate whether such a MDS can still work efficiently when the nodes' behavior is heterogeneous.

The remainder of this paper is structured as follows: In Section II, we introduce our system model and our detection scheme. An extensive evaluation is presented in Section III. Finally, in Section IV we describe our conclusions.

II. System Model and Architecture

The examined hybrid network consists of buses, trams, pedestrians and a stationary gateway. Buses and trams move within the whole metropolitan area measuring air pollution and sending the collected data to a gateway. The gateway is a stationary node which is responsible for gathering the air pollution data and sending it to the data center for further analysis. Pedestrians with smartphones walk around in the city. They have the ability to generate their own messages and forward other buses', trams' or pedestrians' messages.

We assume the DTN hardware installed in buses and trams is similar to the equipment used in the Optracom project (see Figure 2). The current generation of these nodes are equipped with a Global Positioning System (GPS) receiver, a power supply, a specialized environmental sensor and a DTN board running embedded Linux (OpenWRT) with IEEE 802.11 (WiFi) transceivers. The sensor is responsible for measuring air pollution data, the DTN board combines this data with GPS positioning information and a timestamp and sends this data using the IBR-DTN Bundle Protocol implementation [11]. With such a system it would be easy to integrate pedestrians using smartphones as they could run the Android version of IBR-DTN [5] to communicate with the vehicular nodes.

A. Attack Model

Although buses and trams run on fixed paths, traffic congestion makes individual contacts between buses and trams unpredictable. Hence, buses and trams should not waste any contact but try to forward their messages whenever there is an opportunity. If there are any faulty buses or trams which cannot send or forward data, the system should detect them to notify the operator. Additionally, if the communication system of a bus or a tram is penetrated by attackers, the other nodes also want to detect this as soon as possible to avoid wasting resources by relaying to uncooperative nodes.

Pedestrians with smartphones are individual entities that can make independent decisions regarding the forwarding or deletion of messages. Some of the pedestrians may be defective or even malicious. The most common failure mode is a blackhole attack. Blackhole attackers drop all messages they receive instead of forwarding them. Our system will focus on detecting and mitigating blackhole attackers, which may either be the result of a deliberate attack or the result of hard- or software failures.

B. Misbehavior Detection System

The applied MDS is an encounter record-based reputation system. Encounter record-based means, after two nodes met and exchanged messages, a data structure describing the encounter is created and mutually signed by both parties. In our system this encounter record (ER) has the following format:

$$\begin{aligned} ER &= ID_i, ID_j, sn_i, sn_j, t, Re_{i\to j}, Re_{j\to i} \\ Re_{i\to j} &= \{(msg_{id}, msg_{src} | i \text{ sent msg to } j)\} \\ Re_{j\to i} &= \{(msg_{id}, msg_{src} | j \text{ sent msg to } i)\} \\ sig_i &= E_{RK_i}\{H(ER)\} \\ sig_j &= E_{RK_j}\{H(ER)\} \\ ER^* &= ER, sig_i, sig_j \end{aligned} \quad (1)$$

Collected ERs will be stored in nodes' memory and exchanged upon each contact. They provide provable information about a node's behavior in the past. Most importantly an ER contains sequence numbers (*sn*), the timestamp and IDs of exchanged messages (Re sets). The timestamp and sequence number information can be used to detect most basic manipulations such as omitting or dropping ERs. The 2-tuples (id, src) in the Re set stores the sent message's id and the id of the originating node. The whole record is cryptographically signed by both nodes (sig_i,sig_j). For details about these checks, refer to [8].

The exchanged and collected ERs are used to assess and weigh the behavior of nodes against each other. Based on the ER information the system changes a node's trust reputation (TR), which will ultimately lead to a node being excluded from the network if its TR gets too low. Two indicators are calculated from the Re set in the ERs to characterize a node's behavior. The *Message Forwarding Ratio* θ is defined as

$$\theta = \frac{\sum_{m=0}^{m<w} N_{forwarded}^{ER_m}}{\sum_{m=0}^{m<w} N_{received}^{ER_m}} \quad (2)$$

$N_{forwarded}^{ER_m}$ indicates the number of messages forwarded to other nodes, but not originated from this node. $N_{received}^{ER_m}$ indicates the number of messages received but not destined for this node in the encounter record ER_m. A bigger θ indicates a cooperative node, while a smaller θ implies selfishness.

The second metric is the *Message Receiving Ratio* ψ which is defined as

$$\psi = \frac{\sum_{m=0}^{m<w} N_{received}^{ER_m}}{received_{unique}} \quad (3)$$

ψ is the ratio between received messages and the number of unique message IDs received. $N_{received}^{ER_m}$ is defined similarly

异常监测 更合理的方法

to the definition in θ, while $received_{unique}$ is the number of *unique* messages received by this node:

$$received_{unique} = |\{msg_{id} \mid \forall\, msg_{id} \in ER.Re_{i \to j}\}| \quad (4)$$

The rationale is, that when a node receives msg_{id} n times because it keeps dropping that message, its $N^{ER_m}_{received}$ will increase n times while its $receive_{unique}$ will increase only by 1. For a perfectly behaving node without buffer pressure the best achievable value is $\psi_{opt} = 1$. Malicious nodes dropping messages will have higher ψ ratios.

Each node will calculate θ and ψ of encountered nodes and subject them to k-means clustering trying to separate normal behavior from malicious behavior. To prevent false positives, the system makes sure to only punish or reward nodes that clearly exhibit malicious or exemplary behavior by modifying their TR ratings. The TR of nodes, whose behavior does not show a clear trend, will not be modified. The clustering algorithm and subsequent rules to modify the TR are detailed further in [10], where they have proven to adapt successfully to different scenarios, with homogenous nodes.

The question we are interested in this work is, whether this approach is still suitable when there are nodes with widely varying characteristics such as the movement or communication patterns within a single system.

III. Performance Evaluations

A. Simulation Setup

We use the DTN simulator *The ONE* [12] in version 1.4.1 to evaluate the system. The simulated time is 12 hours. Each node has 1 GB buffer size, a transmission radius of 50 meters and a transmission rate of 250 kB/s. Each message has a lifetime of 45 minutes and a size between 500 kB and 1 MB. We performed comparative measurements using the Epidemic [13], MaxProp [3], PROPHET [14] and Spray and Wait [15] routing protocols. Unless otherwise noted, the simulation results presented for each scenario are the average, min and max results of 10 experimental runs.

We simulate the Braunschweig public transportation system. The system consists of 54 stops and 28 buses and trams running on 13 assigned lines. Vehicles move with a speed between 9.72 km/h and 50.04 km/h. In an interval between 25 and 30 seconds, a randomly chosen vehicle generates one air pollution message which is sent to the gateway. The gateway, located near the Braunschweig main station, receives those messages. We add 280 pedestrians with a moving speed varying from 3.75 km/h to 5.43 km/h using the Random Waypoint movement model.

B. Pedestrians Supporting the VDTN

As lined out in section I, we consider an application where vehicles gather environmental data and send it to a gateway. In this experiment we will check the effects of adding pedestrians to the system and compare the performance to a system using vehicles alone.

The delivery rate is an indication of the service quality in VDTNs. Figure 3 presents the delivery rates for five different scenarios using four different routing protocols. In all five scenarios, only vehicles generate messages and send them to the gateway. In the first and fifth scenarios there are only vehicles in the system, and we evaluate the delivery rates with 100% benign vehicles and 20% malicious vehicles respectively. In the other scenarios, pedestrians are added to the system to help forwarding the messages. None, 50% or 100% malicious pedestrian nodes are chosen to evaluate the pedestrians' effects on network performance.

The results depicted in Figure 3 show that, in the first scenario when there are only vehicles in the network, they achieve delivery rates of 87%, 95%, 84%, 78% for Epidemic, MaxProp, PROPHET and Spray and Wait respectively. When we add 280 benign pedestrians to the network, the delivery rates for Epidemic and MaxProp increase. Even with 50% malicious pedestrian nodes, the system still sustains a higher delivery rate for Epidemic and MaxProp. In these cases, only when 100% of the pedestrian nodes are malicious nodes, the delivery rates decrease because these malicious nodes replace some communicating opportunities between vehicles while dropping all received messages.

The results obtained from Epidemic and MaxProp show, that the network performance can be improved with the help of pedestrians. However, when using PROPHET or Spray and Wait, adding pedestrian nodes decreases the delivery rates. The reason for PROPHET's performance is that it is designed to cope with non-random mobility models. When there are only vehicles in the network, PROPHET can achieve a good delivery rate because of the repeating behavioral patterns of buses and trams. However, with randomly moving pedestrians, PROPHET has difficulties predicting good forwarding nodes, hence the delivery rates decrease.

The problem for Spray and Wait is, that this protocol limits the number of replicas for a given bundle. Giving one of the limited bundle copies to a vehicle is normally a good idea, as vehicles travel faster and by design the bus and tram lines usually cover a large area. However, if a pedestrian gets a copy, he moves much slower and might not cover a large area due to the Random Waypoint movement model. Thus, there is a higher chance for a bundle to get "stuck".

We also checked the delivery rates when there are 20% of malicious vehicular nodes in the network. This decreases delivery rates significantly in all cases. This shows the relative importance of the vehicles in the examined scenario.

Overall we see, that with a suitable routing protocol, pedestrians can be used to improve the performance of the system. Even a substantial amount of misbehavior in the pedestrian nodes will at least not hurt the performance in term of delivery rates. Misbehavior in the vehicles on the other hand is more critical, and should be detected reliably.

Another important performance metric is the latency. Figure 4 presents the latency for the five different scenarios using four different routing protocols. We see that with Epidemic and MaxProp the 280 additional pedestrians decrease latency, even with 50% malicious pedestrian nodes. Using Epidemic and MaxProp, the latency with 280 benign pedestrians joining the

实验的几种图 检测/性能 可以参考~

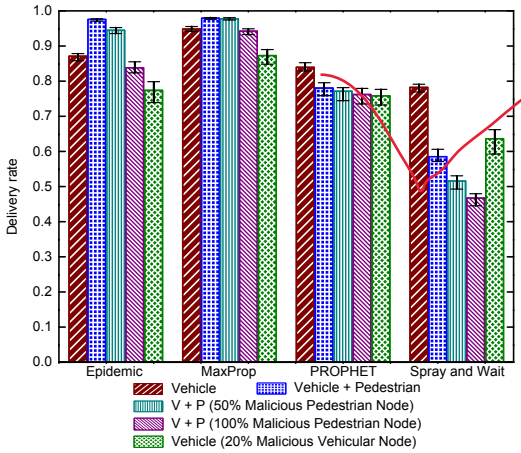

Figure 3. Delivery rate in the VDTN

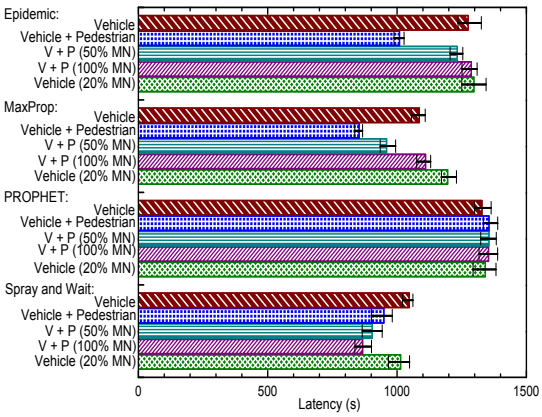

Figure 4. Latency in the VDTN

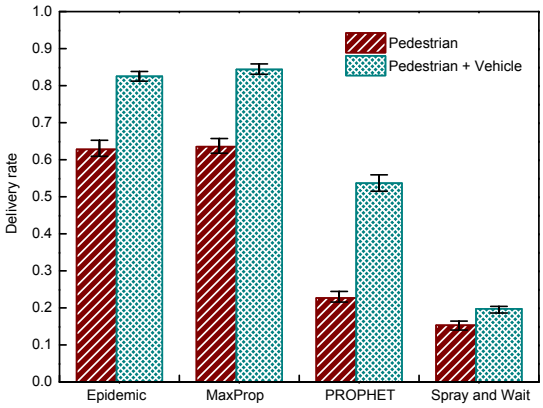

Figure 5. Delivery rate in the smartphone-based DTN

network, is shorter than the latency when only vehicles exist in the network. Only with 100% malicious pedestrian nodes the latency increases a bit. As in the delivery rate experiments, 20% malicious vehicular nodes have a more severe effect and affect the latency negatively.

As seen in the delivery rate results, PROPHET does not cope very well with the random mobility model, hence the latency when random pedestrian nodes join the network increases.

Interestingly, with pedestrians joining in the network, the latency time using Spray and Wait also decreases. However, this does not imply higher performance: Keep in mind, that with Spray and Wait the delivery rate decreased significantly with additional pedestrians. Spray and Wait [15] implements a mechanism that distributes a fixed, limited number of copies first and then waits for one of the relays encountering the destination. Since giving one of the bundles to a random moving pedestrian that might not cover much mapping area, is an inferior choice to giving that bundle to a vehicle exhibiting fast and directed motion, the delivery rate decreased. On the other hand, this implies that only the "easy" bundles get delivered in this scenario: Either the bundle is generated near the gateway from a network topology point of view, or it has a high chance of getting lost due to the limited lifetime. Therefore the average latency for the bundles that actually do arrive decreases.

C. Vehicles Supporting the Smartphone-based DTN

We also looked into the effects of a hybrid DTN from the perspective of the mobile users: Considering there is already a smartphone-based opportunistic network, where users can communicate with each other, the question is why they should cooperate with vehicular nodes. As the environmental monitoring scenario is a pure machine-to-machine application there is no immediate benefit for mobile users acting as data mules as we assumed in the previous section. However, if we assume a tit-for-tat strategy where vehicles also transmit users' data, there might be enough incentive for mobile users to cooperate. Therefore, in this section we will evaluate whether the vehicles can improve the quality of service for applications running in the smartphone-based DTN.

As before our network consists of 28 vehicles and 280 pedestrians. In an interval between 15 and 25 seconds, a randomly chosen pedestrian generates one message for another pedestrian. That means in this experiment we have a real P2P communication pattern, compared to the sink-based network from the Optracom scenario in the previous section.

Figure 5 shows the delivery rates using four different routing protocols. When only the pedestrians exist in the mobile network, the delivery rates are 63%, 64%, 23%, 15% for Epidemic, MaxProp, PROPHET and Spray and Wait respectively. In all scenarios, with the help from the vehicles, the delivery rates increase significantly, achieving 83%, 84%, 54%, 20% for the same routing protocols. When looking at the latency in Figure 6 we see, that even with the higher delivery rates the average latency decreases in all scenarios. These results show that the vehicles are able to shorten the latency of the successfully forwarded messages and lead to a better service quality. Overall these results show that for the pedestrians, the cooperation from the vehicles is a significant advantage, which is a strong incentive for them to also help the vehicles in return.

D. MDS Performance

We look at the performance of the misbehavior detection in the network. As seen from the performance evaluations

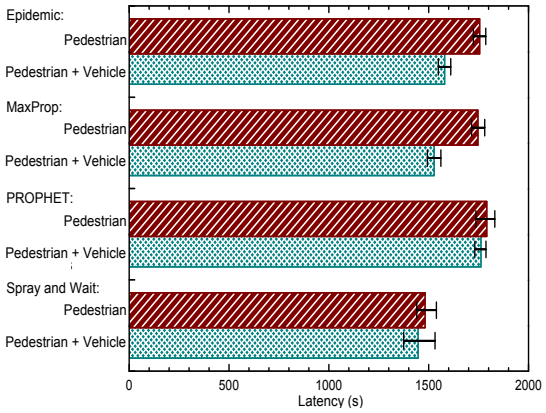

Figure 6. Latency in the smartphone-based DTN

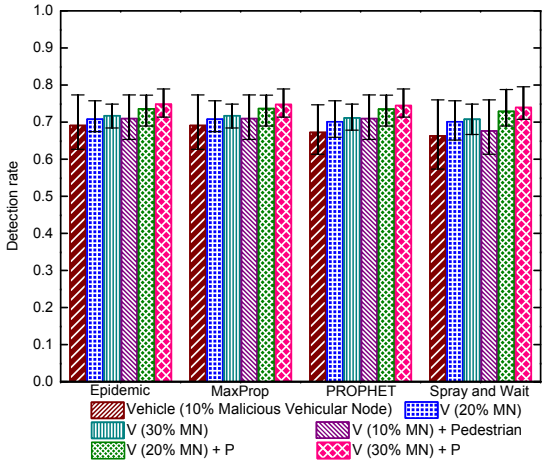

Figure 7. Malicious vehicle detection rate with and without pedestrians

in section III-B, it is crucial to detect misbehaving vehicles, while misbehaving pedestrians have only little impact on the system. As metric we use the average detection rates. We define the detection rate as the percentage of malicious nodes that have been detected by *all* good nodes. For a detection rate of 100%, we require that *all* malicious nodes are detected by *all* normal nodes. This is a very hard metric, as usually this is not necessary for flawless system operation. If two nodes never met, or do not have messages to exchange, the advantage of knowing that a specific node is malicious is limited. The detection rate is defined as:

$$d\_rate = \frac{\#true\_positive}{\#normal\ nodes \times \#malicious\ nodes} \quad (5)$$

where a true positive is defined as the correct detection of one malicious node by one of the benign nodes.

From our previous work in [10], we already know, our MDS has a good performance detecting malicious nodes in a purely vehicle-based network. The question we want to answer here is, whether the system can keep up this performance with lots of pedestrian nodes exhibiting different characteristics compared to the vehicles in the network. The results of this test can be seen in Figure 7. For every routing protocol we performed a simulation with only the vehicles, and a second one where 280 pedestrians join the network. For each simulation we evaluated 3 situations where we randomly choose 3, 6 and 9 vehicles (10%, 20%, 30%) among the 28 vehicles as blackhole attackers.

It can be seen, that our MDS can achieve a detection rate of around 70% for all routing protocols when no pedestrian nodes are present. 70% is actually a very good result, as our definition of detection rate is very strict: A malicious node needs to be detected by *all* other nodes to count as "detected". However, in the Braunschweig system, some of the buses or trams never meet each other, hence the detection rate cannot achieve 100%. The more often a node meets an attacker, the higher the chance it will detect the offender. So despite a lower detection rate according to the strict definition, the system is still immunized pretty well against offenders.

In the second case we added the pedestrians which are also generating messages. To get comparable values, all pedestrians are benign, but we still choose 10%, 20% and 30% of the vehicles as blackhole attackers. The results of this scenario are also shown in Figure 7. We see that the MDS can sustain a detection rate of around 70% even though pedestrians participate in the network. Nodes with different patterns do not affect the ability of the MDS to discriminate between good and malicious behavior. This shows, that the clustering-based self-balancing MDS can not only adapt to different scenarios but can also deal with group heterogenous nodes with different movement and communication patterns.

While we have seen that malicious pedestrians can be tolerated, we want to check, whether they can be detected by the MDS. Generally this is a hard task, as an attacker can usually only be identified if several combined observations provide enough evidence to classify him as malicious. With a high number of slow moving pedestrians, some of them might only be contacted a few times or not at all. In Figure 8 we see the result of a scenario where 50% of the pedestrians are malicious. Again the amount of malicious vehicular nodes is varied between 10% and 30%. Figure 8 presents two kind of detection results: How many malicious vehicles are detected by the vehicles and how many malicious pedestrians are detected by the vehicles. As in the previous results with benign pedestrians, still around 70% of the evil vehicles are detected. For Epidemic, MaxProp and PROPHET around 18% of the pedestrian attackers can be detected and 11% for Spray and Wait.

These are good results. As evil vehicles have a more severe effect on the network performance they should be reliably detected. The MDS is able to do this no matter there are benign, malicious or no pedestrians at all. As expected, the detection rate of vehicles detecting pedestrians is not as high as the detection rate of vehicles detecting other vehicles. The reason is, that our MDS needs to learn and can only make a judgement relying on frequent encounters. However, vehicles do not meet all of the pedestrians. While the detection rate of vehicles detecting pedestrians is not so high, pedestrians more frequently in contact with the vehicles or even following

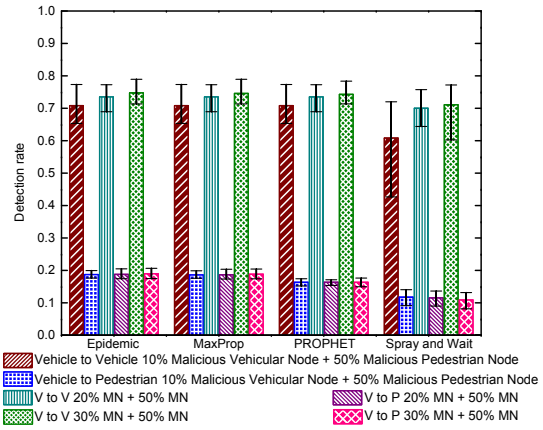

Figure 8. Detection rate in the hybrid VDTN

vehicles actively trying to disrupt the network, have a higher chance of being detected by the MDS.

In fact, we think the small but significant pedestrian detection rate can have a good effect in a real system: Remember, that a smartphone-based DTN means, there are some users behind those phones who want to use the network service. Also, as we have seen in section III-C, it is desirable for pedestrians to rely on vehicles to achieve a higher service quality. While the experiment shows that *most* of the time a malicious pedestrian is not detected, there is still a *significant* chance of being detected. The more frequently an attacker interacts with the system, the higher the chance of detection. From a user's perspective the chance of being detected can be seen as similar to the chance of getting a speeding ticket: Most of the time you can exceed the speed limit without being detected. But there is still a non-negligible chance of being caught and punished, that provides enough incentive for most drivers not exceeding the speed limit too often. Similarly we think, the risk (up to 18%) of cheating the hybrid VDTN system for selfish reasons would be considered too high by most smartphone users, leading to less misbehaving nodes.

IV. Conclusion

We presented a hybrid VDTN system, which consists of buses and trams running a machine-to-machine sensing application and pedestrians with private smartphones. We show, that both groups can profit from cooperation: Vehicles can obtain higher delivery rates and larger network capacities, especially when transferring bulk messages. Interestingly, this is independent of the fact that there might be large number of misbehaving mobile users. Mobile users get significantly better service quality due to the speed and covered area of the vehicles. While not the focus of this work, we have seen that not all routing protocols are equally suitable for this kind of the heterogeneous DTNs. Probably it might be a good idea to use different kind of cooperating routing protocols for the different parts of the network.

For the environmental monitoring scenario reliability is a key metric, thus the system should be protected by a MDS. We have shown this can be done with an encounter record-based self-balancing MDS. The important point is, that the MDS's learning and balancing mechanisms still work correctly when dealing with two groups of nodes with widely different behavior. While technically misbehaving mobile users cannot harm the system performance much, when a significant number of misbehaving users are detected by the MDS, it can provide a strong incentive for mobile users to cooperate.

The results presented in this paper show that vehicular networks and mobile DTNs consisting of the evermore ubiquitous smartphones should be combined, as this can provide better service for both systems without compromising the integrity of either system.

融合多个子网 形成的OppNet:
1.强规律(相位/频率)/有桩自行车
2.不停的周期/公交地铁
3.快速穿越不同的区域/vehicle
4.小范围"无规则"移动/行人

用不同的 路由算法 在不同的子网 运行

随机性强的/规律性强的/
位置方向有效的/社会属性有效的/
副本控制散布方案有效的/概率估计有效的

References

[1] A. Pentland, R. Fletcher, and A. Hasson, "Daknet: rethinking connectivity in developing nations," *Computer*, vol. 37, no. 1, pp. 78–83, Jan. 2004.

[2] S. Guo, M. H. Falaki, E. A. Oliver, S. Ur Rahman, A. Seth, M. A. Zaharia, and S. Keshav, "Very low-cost internet access using kiosknet," *SIGCOMM Comput. Commun. Rev.*, vol. 37, no. 5, pp. 95–100, Oct. 2007.

[3] J. Burgess, B. Gallagher, D. Jensen, and B. N.Levine, "MaxProp: Routing for Vehicle-Based Disruption-Tolerant Networks," in *Proc. IEEE INFOCOM*, Barcelona, Spain, Apr. 2006.

[4] S. Lahde, M. Doering, W.-B. Poettner, G. Lammert, and L. Wolf, "A practical analysis of communication characteristics for mobile and distributed pollution measurements on the road," *Wireless Communications and Mobile Computing*, vol. 7, no. 10, pp. 1209–1218, Dec. 2007.

[5] J. Morgenroth, S. Schildt, and L. Wolf, "A bundle protocol implementation for Android devices," in *Proceedings of the 18th Annual International Conference on Mobile Computing and Networking - Mobicom '12*, New York, USA, Aug. 2012, p. 443.

[6] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, Boston, USA, Aug. 2000, pp. 255–265.

[7] S. Buchegger and J.-Y. L. Boudec, "Performance analysis of the CONFIDANT protocol," in *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing*, Lausanne, Switzerland, Jun. 2002, pp. 226–236.

[8] Y. Guo, S. Schildt, and L. Wolf, "Detecting blackhole and greyhole attacks in vehicular delay tolerant networks," in *the Fifth International Conference on Communication Systems and Networks*, Bangalore, India, Jan. 2013, pp. 1–7.

[9] F. Li, J. Wu, and A. Srinivasan, "Thwarting blackhole attacks in disruption-tolerant networks using encounter tickets," in *INFOCOM 2009, IEEE*, Rio de Janeiro, Brazil, Apr. 2009, pp. 2428–2436.

[10] Y. Guo, S. Schildt, T. Pögel, and L. C. Wolf, "Detecting Malicious Behavior in a Vehicular DTN for Public Transportation," in *Global Information Infrastructure and Networking Symposium 2013 (GIIS'13)*, Trento, Italy, Oct. 2013, pp. 1–8.

[11] S. Schildt, J. Morgenroth, W.-B. Pöttner, and L. Wolf, "IBR-DTN: A lightweight, modular and highly portable Bundle Protocol implementation," *Electronic Communications of the EASST*, vol. 37, pp. 1–11, Jan. 2011.

[12] A. Keränen, J. Ott, and T. Kärkkäinen, "The ONE simulator for DTN protocol evaluation," in *Proceedings of the 2nd International Conference on Simulation Tools and Techniques*, Rome, Italy, Mar. 2009, pp. 55:1–55:10.

[13] A. Vahdat and D. Becker, "Epidemic routing for partially-connected ad hoc networks," Duke University, Tech. Rep., 2000.

[14] A. Lindgren, A. Doria, and O. Schelén, "Probabilistic routing in intermittently connected networks," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 7, no. 3, pp. 19–20, Jul. 2003.

[15] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Spray and wait: An efficient routing scheme for intermittently connected mobile networks," in *Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking*, Philadelphia, USA, Aug. 2005, pp. 252–259.